XSEDE Security Working Group Service Provider (SP) Guide & FAQ

September 12, 2013

Version 0.1.1

Table of Contents

A. Document History

Relevant Sections	Version	Date	Changes	Author
Entire Document	0.1.1	9/12/2013	Baseline	A. Slagell

B. Document Scope

XSEDE is a large, distributed enterprise with complex procedures and policies. This guide is intended to assist new security personnel who are joining the *XSEDE Security Working Group* (XSWoG) to understand the policies and procedures in-place.

C. Document Body

C.1. The XSEDE Security Working Group (XSWoG) FAQ

C.1.1. What is the XSWoG?

Created with the XSEDE Security Working Group Charter [1], the following definition for the XSWoG comes from the XSEDE Level 1 Service Provider Baseline Security Standard [2]:

This group is responsible for creating security policies and procedures to be approved by the XSEDE Advisory Board, as well as helping to realize the goals set forth for XSEDE security operations. At a minimum, this group has the XSO, funded members of XSEDE security operations, and a representative from each Level 1 Service Provider (SP). Additional representatives and service providers may join upon approval of the XSO.

C.1.2. How do I contact XSWoG members?

All members of the XSWoG have access to a shared wiki where individual contact information can be found [3]. To reach all XSWoG members, non-sensitive information can be sent to the ops-security@xsede.org mailing list. The XSWoG chair and XSEDE Security Officer can be reached at security-lead@xsede.org.

C.1.3. What do I do in case of a security emergency?

Please refer to the XSEDE Security Playbook [4] for specific instructions and a flow chart. Emergency contact information for individuals is available on the incident response wiki at [3].

There is a hotline that can be used 24 hours a day. This number is known to each site's Security Working Group lead. New sites should contact the Security-WG chair or XSEDE Security Officer for this information.

C.1.4. Typical XSWoG Topics & Tasks

The XSWoG focuses on a broad range of coordination, response, and planning efforts. Ongoing work involves policy and procedure development as well as coordinating emergency incident response.

Typical projects coordinated by the Security-WG include pilot projects (e.g., OTP, science gateway authorization schemes, vulnerability management planning, etc.) as well as general processes such as review of certificate authorities and conducting risk assessments.

Documents that have been drafted to date by the XSWoG include the:

- XSEDE Security Working Group Charter [1]
- XSEDE Security Playbook [4]

- XSEDE Level 1 Service Provider Security Agreement (draft) [2]
- XSEDE Level 1 Service Provider Baseline Security Standard [5]
- XSEDE Acceptable Use Policy [6]
- XSEDE Community User Accounts Policy (draft) [7]
- XSEDE Security Working Group Newbie Guide & FAQ
- XSEDE Security Risk Assessment Final Report [8]

C.1.5. Mailing Lists

XSEDE Security Working Group (ops-security@xsede.org)

To become a member of the XSWoG, and hence on this list, you must be a security representative from a XSEDE site. To request to be added to the mailing list, send email to the Security-WG lead at security-lead@xsede.org or work through your local site's primary XSWoG representative.

*Incident Discussion List (incident-discuss@xsede.org) ** **Encrypted List** **

The primary purpose for this list is to announce Incident Response meeting details and share "non-critical" Incident Response information with the XSEDE Incident Response team. This is a sub-team for the XSWoG for those actually involved in their institution's incident response. To be added to the incidents announce list and get the relevant encryption keys, send email to the Security-WG lead at security-lead@xsede.org or work through your local site's primary XSWoG representative.

*Incident Report (incident-report@xsede.org) ** **Encrypted List** **

This list is used to communicate critical security event information that requires immediate attention of the XSEDE Incident response team. Because mail sent to this list may trigger emergency notification and escalation action, it should only be used for security emergencies that directly affect the XSEDE project. Subscription to this list is determined by the Incident Response contact per site as detailed in the XSEDE Security Contact List [3].

Security-WG Chair (security-lead@xsede.org)

Email will be sent to the Security-WG Chair and XSEDE Security Officer and Level III Operations manager.

C.1.6. Email Encryption

Sensitive email sent to the incidents lists must be encrypted using a private, symmetric PGP/GPG key. Details can be obtained from the XSWoG chair or XSEDE Security Officer (XSO).

Email to individual XSWoG members may be encrypted using their PGP keys. Keys are regularly exchanged and signed at XSWoG face-to-face meetings and can also be obtained from key repositories with proper verification. The XSWoG chair and XSO should sign all member keys to make verification simpler.

C.1.7. Teleconferences

XSEDE Security-WG call

Currently, a weekly call is used for coordination and communication, with participation expected from all members Level 1 service providers. Planning activities, policy, current project updates, and security issues are discussed during these calls. Please contact the Security Working Group lead for the phone number and scheduling information (security-lead@xsede.org).

Weekly Incident Response call

A weekly call for Level 1 SP incident responders is used to review current security incidents and emerging threats. Discussion of tools, vulnerabilities, mitigations and detection methods are typical.

C.2. XSEDE Security Working Group Resources

C.2.1. XSEDE Staff Wiki

Current projects, meeting minutes and draft documents are kept in the Security Operations section of the staff wiki [9].

C.2.2. XSWoG Secure Wiki

The XSWoG uses a secure site [10] for incident documentation and other sensitive information. All XSWoG members should have access. If not, they can request it through their local SP's primary security representative.

C.2.3. XSWoG Secure IM Service

The XSWoG uses a secure jabber service for information sharing and incident response coordination. Configuration information can be found on the XSWoG Wiki [10]. Jabber accounts can be requested through your local SP's primary security representative who can contact the security leads at security-lead@xsede.org.

C.3. XSWoG Expectations

As noted in the XSEDE Level 1 Service Provider Agreement [2], SPs are expected to participate in the XSWoG and to make appropriate security and emergency contact information available for inclusion in the XSWoG contact lists. Additional responsibilities include those outlined in the following documents:

- XSEDE Level 1 Service Provider Security Agreement [2]
- XSEDE Level 1 Service Provider Baseline Security Standard [5]

Security staff should also be aware of:

- XSEDE Security Working Group Charter [1]
- XSEDE Security Playbook [4]
- XSEDE Acceptable Use Policy (draft) [6]
- XSEDE Security Risk Assessment Final Report [8]

In addition to understanding the above responsibilities, new sites are expected to participate in XSWoG activities and incident response coordination by:

- Attending and participating in XSWoG meetings, projects and tasks;
- Maintaining site Security/Incident Response points of contact;
- Participating in weekly incident response calls;
- Responding to security advisories issued by the XSWoG in a timely manner; and
- Participating in the XSEDE risk assessment process.

C.4. Important XSEDE-specific Software Systems

C.4.1. AMIE (Account Management Information Exchange)

AMIE is an identity and accounting data management and transfer system used by XSEDE to replicate, update, and propagate accounts and accounting data. A security analysis of the AMIE protocol has been done and can be found in [11].

AMIE is typically implemented using a restricted, unprivileged account, which communicates over SSH. The AMIE software itself has not been reviewed for security by XSEDE staff.

C.4.2. Inca

Inca is a flexible framework for the automated testing, benchmarking and monitoring of Grid systems. It includes mechanisms to schedule the execution of information gathering scripts, and to collect, archive, publish, and display data.

The INCA software itself has not been reviewed for security by XSEDE staff.

C.4.3. Other ZSEDE Software & Services

A system characterization of all XSEDE systems, software and other assets was compiled as part of the original XSEDE risk assessment. This can be found on the staff wiki at [12].

C.5. References

[1] XSEDE Security Working Group Charter
https://www.xsede.org/documents/10157/247425/XSEDE+Security+Working+Group+Charter.docx

[2] Draft XSEDE Level 1 Service Provider Security Agreement,
https://www.xsede.org/web/staff/staff-wiki/-/wiki/Main/XSEDE+Security+policies

[3] XSWoG Secure Wiki: Member Contact Info https://ops-security.xsede.org/wiki/XSEDE_Security_Contact_List

[4] XSEDE Security Playbook http://hdl.handle.net/2142/45238

[5] XSEDE Level1 Service Provider Baseline Security Standard, http://hdl.handle.net/2142/45239

[6] Draft XSEDE Acceptable Use Policy, https://www.xsede.org/web/staff/staff-wiki/-/wiki/Main/XSEDE+Security+policies

[7] Draft XSEDE Community User Accounts Policy, https://www.xsede.org/web/staff/staff-wiki/-/wiki/Main/XSEDE+Security+policies

[8] XSEDE Security Risk Assessment Final Report,
https://www.ideals.illinois.edu/handle/2142/44892

[9] XSEDE Staff Wiki: Security Operations, https://www.xsede.org/web/staff/staff-wiki/-/wiki/Main/Security+Operations

[10] XSWoG Secure Wiki, https://ops-security.xsede.org/wiki/Main_Page

[11] AMIE Account Security Evaluation, J. Basney, February 2004.
https://repo.xsede.org/head/account-management/doc/AMIE/

[12] XSEDE Staff Wiki: System Characterization, https://www.xsede.org/web/staff/staff-wiki/-/wiki/Main/XSEDE+System+Characterization